"Express Mail" mailing label number EV 331533759 US

Date of Deposit: January 9, 2004

ATTORNEY DOCKET NO.: 14316US02

AUTHENTICATION OF NOTIFICATIONS RECEIVED IN AN ELECTRONIC DEVICE IN A MOBILE SERVICES NETWORK

CROSS-REFERENCE TO OTHER APPLICATIONS

[0001] The present application claims the benefit of priority of U.S. Provisional Patent Application having serial number 60/438,870, filed on January 9, 2003, and hereby incorporates herein by reference the complete subject matter thereof in its entirety.

[0002] The present application also hereby incorporates herein by reference the complete subject matter of PCT Application having publication number WO 02/41147 A1, and having application number PCT/US01/44034, filed on November 19, 2001, in its entirety.

[0003] The present application also hereby incorporates herein by reference the complete subject matter of U.S. Provisional Patent Application having serial number 60/249,606, filed November 17, 2000, and U.S. Provisional Patent Application having serial number 60/422,048, filed October 29, 2002, in their respective entireties.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0004] [Not Applicable]

[MICROFICHE/COPYRIGHT REFERENCE]

[0005] [Not Applicable]

BACKGROUND OF THE INVENTION

[0006] Electronic devices (i.e., mobile electronic devices having software/firmware), for example, mobile cellular phones, personal digital assistants (PDA's), pagers, MP3 players, digital cameras, etc. often contain firmware and/or application software that are either provided by the manufacturers of the electronic devices, telecommunication carriers, or third parties. These firmware and application software often contain bugs. New versions (updates) of the firmware and software are periodically released to fix the bugs, introduce new features, or both.

[0007] It may be difficult to inform/notify an electronic device of the need to update the device's firmware/software and it may also be difficult to determine whether an update notification received is authentic. An unauthorized, illegal, software hacker may attempt to infiltrate an electronic device management server and send a notification to an electronic device to compel the device to retrieve an unauthorized, spurious update package.

[0008] Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of skill in the art, through comparison of such systems with some aspects of the present invention as set forth in the remainder of the present application with reference to the drawings appended hereto.

SUMMARY OF THE INVENTION

[0009] Aspects of the present invention may be found in a method of updating an electronic device. The method may comprise receiving a notification in the electronic device and determining the authenticity of the notification in the electronic device. The notification may comprise, for example, one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification. The electronic device may comprise, for example, one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

[0010] In an embodiment of the present invention, the method may further comprise informing the electronic device of availability of at least one update package for updating at least one of firmware and software resident in the electronic device and simultaneously informing a notification history server that a notification has been sent to the electronic device.

[0011] In an embodiment of the present invention, determining the authenticity of the notification may comprise contacting a notification history server, the notification history server keeping a record of notifications sent to the electronic device.

[0012] In an embodiment of the present invention, the method may further comprise ignoring the notification in the electronic device upon determining that the notification is inauthentic, recording that an inauthentic notification has been received, and waiting to receive another notification in the electronic device.

[0013] In an embodiment of the present invention, the method may further comprise determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is authentic.

[0014] In an embodiment of the present invention, the method may further comprise retrieving the update package and performing an update of at least one of firmware and software resident in the electronic device.

[0015] In an embodiment of the present invention, determining the authenticity of the notification in the electronic device may further comprise determining whether the notification was sent from an authorized server. An authorized server may comprise one of a management server and a customer care center, for example.

[0016] In an embodiment of the present invention, the notification may comprise location and identification information regarding a management server providing access to an update package and information regarding the update package. The location and identification information may comprise, for example, at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

[0017] In an embodiment of the present invention, the method may further comprise retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification. The address of the default management server may be provisioned in the electronic device during a bootstrap provisioning event. In one embodiment, retrieving the update package from the default management server is performed after authentication of the notification message.

[0018] In an embodiment of the present invention, the method may further comprise retrieving an update package via a download agent in the electronic device and updating at least one of firmware and software in the electronic device via an update agent in the electronic device.

[0019] In an embodiment of the present invention, the method may further comprise preventing unauthorized updates of at least one of firmware and software in the

electronic device. In one embodiment, preventing unauthorized updates may further comprise a notification being sent to the electronic device that may be discernable by an end-user. The end-user may be prompted to initiate an update process. When the end-user initiates the update process, the electronic device may be adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic. Alternatively, the electronic device may permit the update package to be downloaded, if the notification is determined to be authentic.

[0020] In an embodiment of the present invention, preventing unauthorized updates may further comprise receiving a dynamic key component from a management server in the electronic device, accessing a static key component from memory in the electronic device, and instructing a download agent to use the dynamic key component and the static key component to generate a security key. The generated security key may facilitate access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device may be denied access to the update package.

[0021] Aspects of the present invention may be found in a mobile services network. The network may at least comprise at least one electronic device, a management server communicatively linked with the at least one electronic device via a communication link, and a notification history server operatively connected to the management server. The notification history server may comprise a record of authentic notifications sent to the at least one electronic device.

[0022] In an embodiment of the present invention, the electronic device may at least comprise non-volatile memory, a short message entity, random access memory, and security services.

[0023] In an embodiment of the present invention, the non-volatile memory in the electronic device may at least store an update agent, a firmware and real-time operating system, an operating system layer, a download agent or browser, and an end-user related data and content.

[0024] In an embodiment of the present invention, the electronic device may comprise one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

[0025] In an embodiment of the present invention, the electronic device may be adapted to receive notifications informing the electronic device of availability of update packages at the management server. The electronic device may also be adapted to determine the authenticity of the notifications by contacting the notification history server.

[0026] In an embodiment of the present invention, the notification history server may be adapted to determine whether a notification is authentic by examining message identification information in the notifications.

[0027] In an embodiment of the present invention, the electronic device may be adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authentic.

[0028] In an embodiment of the present invention, the electronic device may be adapted to determine whether a notification originated from an authorized sender.

[0029] In an embodiment of the present invention, an authorized sender may be at least one of the management server and a customer care center resident in the network.

[0030] In an embodiment of the present invention, the network may further comprise a short message center adapted to store and forward messages to and from the electronic device. The short message center may be adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages.

[0031] In an embodiment of the present invention, notifications may comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

[0032] In an embodiment of the present invention, the network may further comprise at least one user data field containing message identification information.

[0033] In an embodiment of the present invention, notifications may further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package.

[0034] In an embodiment of the present invention, location and identification information may comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

[0035] In an embodiment of the present invention, upon determining that a notification received in the electronic device is inauthentic, the electronic device may ignore the notification and waits for another notification. A record may also be created recording that an inauthentic notification has been received.

[0036] In an embodiment of the present invention, the management server may comprise the notification history server and an update package repository.

[0037] In an embodiment of the present invention, the notification history server may be incorporated into a short message center in the network.

[0038] In an embodiment of the present invention, the network may further comprise a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device.

[0039] In an embodiment of the present invention, preventing unauthorized updates may comprise that a notification may be sent to the electronic device which may be discernable by an end-user. The end-user may be prompted to initiate an update process. When the end-user initiates the update process, the electronic device may be adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic. Alternatively, the electronic device may permit the update package to be downloaded, if the notification is determined to be authentic.

[0040] In an embodiment of the present invention, preventing unauthorized updates may further comprise receiving a dynamic key component from a management server in the electronic device, accessing a static key component from memory in the electronic device, and instructing a download agent to use the dynamic key component and the static key component to generate a security key. The generated security key may facilitate access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package. Otherwise, the electronic device may be denied access to the update package.

[0041] These and various other advantages and features of novelty which characterize the invention are pointed out with particularity in the claims annexed hereto and that form a part hereof. However, for a better understanding of the invention, its advantages, and the objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to accompanying descriptive matter, in which there are illustrated and described specific examples of an apparatus in accordance with the invention.

BRIEF DESCRIPTION OF THE DIAGRAMS

[0042] **Figure 1** is a block diagram illustrating a mobile services network wherein an electronic device has access to a plurality of services according to an embodiment of the present invention; and

[0043] **Figure 1a** is a block diagram illustrating an exemplary notification message format according to an embodiment of the present invention;

[0044] **Figure 2** is a flow diagram illustrating an exemplary method for an electronic device to receive a firmware/software update package notification according to an embodiment of the present invention;

[0045] **Figure 2a** is a flowchart illustrating an exemplary method for authenticating a notification with end-user involvement according to an embodiment of the present invention;

[0046] **Figure 2b** is a flowchart illustrating an exemplary method of preventing unauthorized downloading of information by an electronic device according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0047] **Figure 1** is a block diagram illustrating a mobile services network wherein an electronic device has access to a plurality of services according to an embodiment of the present invention. An electronic device may be for example, a mobile electronic device having software/firmware, such as, mobile cellular phone handsets, personal digital assistants (PDA's), pagers, MP3 players, digital cameras, etc.

[0048] **Figure 1** illustrates a mobile services network 105 wherein an electronic device, for example, mobile handset 107, may be provided access to a plurality of services including a firmware/software update service. The electronic device may also receive notifications, such as short message service (SMS) notifications, of the availability of update packages. An update package may comprise firmware/software updates that modify or change the version of a particular firmware/software, for example upgrading to a newer version. An update package may also add new services to the electronic device or delete services as desired by the service provider or an end-user.

[0049] In response to the notifications, the electronic device may confirm the authenticity of received notifications before initiating download of an update package from a management server 109 via a communications link 143. The mobile services network 105 may comprise an electronic device, for example, mobile handset 107, short message center (SMC) 129, management server 109, notification history server 131, customer care center 135, and update package repository 133.

[0050] The electronic device, e.g., mobile handset 107, may comprise non-volatile memory 111, random access memory (RAM) 125, security services 123, and short message entity (SME) 127. The non-volatile memory 111 of the electronic device may comprise update agent 113, firmware and real-time operating system (RTOS) 115, operating system (OS) layer 117, download agent or browser 119, and end user related data and content 121.

[0051] The electronic device, e.g., mobile handset 107, may receive notifications informing the device of the availability of update packages at the management server 109. Such notifications may originate from either management server 109 or customer care center 135. In response to such notifications, the electronic device may authenticate notifications by contacting notification history server 131.

[0052] Notification history server 131 may maintain details of notifications sent to the electronic device, e.g., mobile handset 107. Once the electronic device determines that a received notification is authentic, i.e., originated from an authorized sender, for example, customer care center 135, the electronic device may download an update package from the update package repository 133 employing the download agent or browser 119 in the electronic device. Subsequently, the electronic device may employ update agent 113 to update the firmware/software, etc. in the electronic device, e.g., mobile handset 107.

[0053] **Figure 1a** is a block diagram illustrating an exemplary notification message format according to an embodiment of the present invention. In **Figure 1a**, notification message 100a may comprise an update flag 110a, or some other type of flag identifying the purpose of the notification, for example a delete flag, modify flag, etc. Additionally, the notification may also comprise at least sender information 120a, end-user information 130a, a universal resource locator 140a or some other type of address information, schedule information 150a, and a dynamic key component 160a, etc.

[0054] The sender information 120a may comprise information corresponding to the server sending the notification and particulars related to the type of modification/update being offered by the notification. The end-user information 130a may comprise a code relating to the electronic device or personalized greetings, etc.

[0055] The universal resource locator 140a may alternatively be an internet protocol address or other type of address. The schedule information 150a may comprise a date and time for which the update/modification may be made available for a particular electronic device or geographical region. The dynamic key component 160a will be

discussed in more detail below. Although the above named exemplary notification information categories (110a-160a) have been illustrated and described, other different notification information categories may be included in notification messages as desired or necessary.

[0056] Referring back to **Figure 1**, short message center (SMC) 129 may be adapted to store and forward messages to and from the electronic device, e.g., mobile handset 107. Short message entity (SME) 127 may be located in a fixed network or alternatively in the electronic device to receive and send short messages. When instructed by management server 109 or customer care center 135, SMC 129 may send notifications to the electronic device regarding availability of update packages, along with other additional related information.

[0057] The electronic device may monitor such notifications and determine whether the notifications are related to update activity. The electronic device may ascertain the validity of received notifications by contacting notification history server 131 and verifying that the notifications were indeed sent by an authorized server/sender, for example, management server 109 or customer care center 135. The electronic device may download an associated update package once the notification has been verified.

[0058] In an embodiment according to the present invention, the user data field of a received SMS message may contain message identification information which may be employed by the electronic device to determine whether a notification received originated from an authorized source, for example, management server 109, or an unauthorized source, for example, an unauthorized server trying to compel the electronic device to retrieve a spurious update package.

[0059] The electronic device may send message identification information retrieved from the notification to notification history server 131 to determine whether the notification history server 131 has a record of such a notification. If the notification history server 131 confirms knowledge of the notification, then the electronic device may download an associated update package and perform an update of the firmware/software,

etc. However, if notification history server 131 is unable to confirm knowledge of the notification based upon the message identification information received from the electronic device, then the electronic device may ignore the received notification and continue normal processing.

[0060] In an embodiment according to the present invention, management server 109 instructs SMC 129 to send an SMS notification to the electronic device. The SMS notification may contain, for example, unique message identification information, a reference to an update package encapsulated as a universal resource locator (URL), or some other information. The management server 109 may also simultaneously inform notification history server 131 of the notification being sent to the electronic device.

[0061] The electronic device may receive the SMS notification containing the unique message identification information, etc., and may then contact the notification history server 131 to determine the authenticity of the received notification. After determining that the notification is authentic, (i.e., the notification originated from an authorized server/sender, for example, management server 109), the electronic device may subsequently download the update package employing, for example, a URL provided in the notification.

[0062] **Table 1** below illustrates an exemplary notification table recording notifications encountered by an electronic device is illustrated below.

Table 1

Notification History Server
Notification Table

Time Stamp	Notification Type	Server Sender Address	Verified	Electronic Device ID
091109192003	modify software	www.sample1.com	yes	abc1
111510062003	update software	www.sample1.com	yes	abc2
122910102003	modify software	www.sample1.com	yes	abc3
101110302003	modify software	www.fraud1.com	no	abc1
000611012003	delete software	www.virus1.com	no	abc3
142911292003	modify software	www.sample1.com	yes	abc2
181612012003	update software	www.sample1.com	yes	abc2
221012152003	delete software	www.virus1.com	no	abc2
091712272003	modify software	www.fraud1.com	no	abc3
103101012004	Update software	www.sample1.com	yes	abc1

Table 1 above discloses numerous entries recording notifications received by an electronic device and the resolution of those notifications.

[0063] In **Table 1** above, numerous notifications received by a plurality of electronic devices are illustrated. The values in **Table 1** are exemplary values, however, numerous other and different values may be provided as desired by security services or end-user demands. When a notification has been received by an electronic device, the electronic device may consult the notification history server to determine whether the notification received is authentic or inauthentic.

[0064] The date/time may be recorded under the heading Time Stamp. The type of notification may be recorded under the heading Notification Type, and the type of notification may comprise an update notification, a modification notification, a deletion notification, etc. The address of the server sending the notification may be recorded under the heading Server Sender Address, and may be an internet protocol (IP) address, universal resource locator (URL), or some other type of identifying address.

[0065] The result of the authentication/verification may be recorded under the heading Verified, and whether the notification, i.e., the sender of the notification is recognized by the notification history server. The identity of the electronic device receiving the notification may also be recorded under the heading Electronic Device ID,

and may be represented by some alpha-numeric code, for example. A plurality of electronic device may be provided authentication of notification services.

[0066] The notification history server may record the time/date when the notification was received, the type of notification that was received, where the notification originated, for example the address of the server sending the notification, and whether or not the notification has been verified as authentic in a table, for example **Table 1**.

[0067] Because hackers may make repeated attempts to infect an electronic device with a virus or steal information from electronic devices and servers communicating with the electronic devices, the notification history server may maintain a record of not only verified servers and their respective addresses, but also unverified servers and their respective addresses. In this way, once a server, i.e., sending address, has been branded hostile, additional notification messages originating from the branded server may immediately be identified as unverified, and thereafter be ignored.

[0068] In an embodiment according to the present invention, the electronic device may request management server 109 to determine whether the notification is authorized. The electronic device may also employ the notification history server 131 to determine the authenticity of the SMS notification.

[0069] In an embodiment according to the present invention, customer care center 135 may send an SMS message to the electronic device employing SMC 129. The SMS message may contain information associated with the update package to be retrieved from update package repository 133 and applied by the electronic device. The customer care center 135 may also cause an entry to be created in notification history server 131 to record that an SMS notification was sent to the electronic device. The electronic device may contact the notification history server 131 to determine the authenticity of the received notification prior to contacting management server 109 to retrieve the associated update package.

[0070] In an embodiment according to the present invention, the SMS message may contain schedule information, identifying when download of an update package should be performed by the electronic device, as part of the notification message.

[0071] In an embodiment according to the present invention, enhanced messaging service (EMS) may be employed by the mobile services network 105 instead of SMC 129. An EMS notification may be sent from an EMS compliant server to an EMS compliant electronic device. EMS is a message transmission service adapted to send a richer/broader message containing combinations of text, simple melodies, pictures (simple, black and white), animations, etc., to an EMS compliant electronic device. EMS technology may extend the user data header (UDH) in SMS. The UDH may be adapted to include binary information in the message header. The UDH may also be applicable in existing services networks without upgrading the network infrastructure. In order for electronic devices to apply EMS technology, the electronic devices, may of course necessarily be EMS compliant.

[0072] In an embodiment according to the present invention, notification of update package availability may be sent using multimedia messaging service (MMS). MMS uses standardized protocols such as, wireless application protocol (WAP), mobile station application execution environment (MExE), and simple mail transfer protocol (SMTP). MMS may also employ a dedicated channel and work complimentarily with an MMS server and MMS user databases.

[0073] In an embodiment according to the present invention, the notification history server 131 and update package repository 133 may be incorporated into management server 109.

[0074] In an embodiment according to the present invention, the notification history server 131 may be incorporated into SMC 129.

[0075] In an embodiment according to the present invention, the notification history server 131 may be part of a broader customer care center 135 for the mobile

services network 105. The customer care center 135 may instruct SMC 129 to send notifications and save information related to the notifications sent, such as message identification information. The customer care center 135 may also provide the saved information to management server 109 to facilitate authenticity verification of notifications.

[0076] In an embodiment according to the present invention, customer care center 135 may send a notification to the electronic device indicating availability of an appropriate update package. The notification may be sent via SMS transport provided by SMC 129. The customer care center 135 may also instruct the notification history server 131 to record that a notification was sent to the electronic device and to associate unique message identification information with the record. The notification may also include message identification information which may be used to verify the authenticity of the notification message.

[0077] The electronic device may contact management server 109 (or another authorized server, if reference to one is provided in the notification message) and use the message identification information to verify the authenticity of the received notification. Management server 109 may respond by confirming the authenticity of the message identification information complimentarily with notification history server 131. The management server 109 may also return a dynamic key component to the electronic device which may subsequently be used as part of a security key for secure communications and access to secure data resources in conjunction with a static key component available in the electronic device, for example an electronic device identifier or end-user identification information.

[0078] The electronic device may receive the dynamic key component and store it in memory, such as RAM 125 or non-volatile memory 111, for subsequent access, usage, and combination with a static security key component, as part of a symmetric or asymmetric security key. The electronic device may also instruct the download agent or browser 119 to use the dynamic key component and the static key component to generate or compute a security key, which may be applied to provide access to download an

update package, for example from update package repository 133 via management server 109. By applying this form of security, data resources on dedicated servers may be protected from unauthorized access while those electronic devices supplying an authorized security key may be provided access to downloadable resources.

[0079] In an embodiment according to the present invention, management server 109 may communicate the dynamic key and a schedule for download of an update package to the electronic device when the electronic device attempts to authenticate a received SMS update package associated notification. For example, an update may be available for download at a particular time, on/after a particular date, or for a particular period of time.

[0080] In an embodiment according to the present invention, an update package associated notification received by the electronic device may include, for example, a URL for a server managing access to the update package, such as management server 109. The electronic device may determine whether the server referred to by, for example, the URL in the notification message, is an authorized server by using known secure identification techniques. If the electronic device determines that the server is an authorized server, then the electronic device may download the appropriate update package employing the download agent or browser 119.

[0081] **Figure 2** is a flow diagram 205 illustrating an exemplary method for an electronic device to receive a firmware/software update package notification according to an embodiment of the present invention. An electronic device may be for example, a mobile electronic device having software/firmware, such as, mobile cellular phone handsets, personal digital assistants (PDA's), pagers, MP3 players, digital cameras, etc.

[0082] In block 207 of **Figure 2,** processing may begin with the electronic device waiting for incoming notifications, such as SMS notifications or other messages. At block 209, the electronic device may receive a notification, such as an update notification via an SMS message.

[0083] At block 211, the electronic device may verify whether the received notification is authentic, i.e., from an authorized source/sender, such as a customer care center 135 or an authorized server, for example, management server 109 using known secure identification techniques. If the electronic device determines that the notification is from an unknown source/sender or an unauthorized source/sender, then, at block 225, the electronic device ignores the received notification and records that a spurious unauthorized notification was received, before resuming processing at block 207.

[0084] If, however, at block 211, the electronic device verifies that the received notification is authentic, then at block 213, the electronic device may determine the URL of the server and update package that provides access to the associated firmware/software update. The notifications may also comprise location and identification information regarding a management server providing access to an update package and information regarding the update package. The location and identification information may also comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

[0085] In an embodiment according to the present invention, the notification may also provide information regarding a location or address of the management server providing access to the update package, along with information about the update package, such as the update version number, etc. The electronic device may also be adapted to ensure that the management server referred to in the notification is an authorized server/sender.

[0086] In an embodiment according to the present invention, if the notification message does not specify a server where a downloadable update may be obtained, the electronic device may retrieve the address of a default management server which may have been previously provisioned in the electronic device (for example, during a bootstrap provisioning event). The electronic device may contact the default management server to retrieve an update package. The notification message may be

authenticated however, prior to contacting the default management server to ensure that the notification was received from an authorized server/sender.

[0087] In an embodiment according to the present invention, the electronic device may contact a default management server whose address is available in the electronic device to determine the address of another server that may be able to provide access to another required update package.

[0088] At block 215, the electronic device may retrieve an update package employing the download agent or a browser (119 in **Figure 1**), or for example, a wireless application protocol (WAP) browser. At block 223, the electronic device may employ the update agent (113 in **Figure 1**) to update the firmware/software in the electronic device using the retrieved update package, before resuming processing at block 207.

[0089] Although an SMS based notification has been described herein, other types of notifications, such as instant messaging (IM), email notifications, (WAP) push messages, etc. are also contemplated. Methods similar to those described herein for verification of authenticity of received notifications may also be employed in other envisioned scenarios.

[0090] In an embodiment according to the present invention, the SMS based notification sent to the electronic device may be viewed by an end-user. The electronic device may also prompt the end-user by displaying a notification message in a display of the electronic device, providing the end-user with an opportunity to explicitly initiate an update process beginning with downloading an update package. Even when an end-user initiates an update process, the electronic device may be adapted to verify the authenticity of the notification before permitting the update package to download, thus providing the electronic device with an added measure of security should the end-user be fooled into initiating a spurious update package download.

[0091] In an embodiment of the present invention, a notification sent to the electronic device may be viewable by an end-user and the end-user may be prompted to

initiate an update process. When the end-user initiates the update process, the electronic device may be adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be fraudulent. The electronic device may also be adapted to permit the update package to be downloaded if the notification is determined to be authentic.

[0092] **Figure 2a** is a flowchart 200a illustrating an exemplary method for authenticating a notification with end-user involvement according to an embodiment of the present invention. In **Figure 2a**, initially an electronic device may be waiting to receive a notification 210a. While waiting to receive a notification the electronic device may be processing normally or performing the function for which the device was designed.

[0093] After some period of time the electronic device may receive a notification 220a. The notification may be discernable by an end-user of the electronic device. The notification may or may not be authentic, i.e., the notification may appear authentic to the end-user, but in reality may be a virus or other malicious, fraudulent notification.

[0094] The end-user may be prompted to initiate an update or modification by the received notification 230a. The end-user may be enticed or tricked into initiating a fraudulent download. The end-user may initiate an update 240a. The electronic device may verify the notification prior to permitting download 250a, even when an end-user has authorized and initiated the download. This provides an additional level of security which may protect the electronic device from malicious or fraudulent activity.

[0095] If the notification is found to be authentic, the electronic device may retrieve the update/modification package 260a and perform the update or modification 270a. However, if the notification is determined to be inauthentic or is unverified, the download procedure is aborted 280a and the notification is ignored. In either situation, retrieval or abort, after completing the task, the electronic device may return to normal processing and wait for further notifications 210a.

[0096] In an embodiment of the present invention, the electronic device comprises a security service preventing unauthorized updating of at least one of firmware and software in the electronic device. In an embodiment of the present invention, a security method may be applied for preventing unauthorized updates of at least one of firmware and software in the electronic device.

[0097] **Figure 2b** is a flowchart 200b illustrating an exemplary method of preventing unauthorized downloading of information by an electronic device according to an embodiment of the present invention. In **Figure 2b**, initially an electronic device may be waiting to receive a notification 210b. While waiting to receive a notification, the electronic device may be processing normally, i.e., performing the function for which the device was designed. After some period of time, the electronic device may receive a notification 220b.

[0098] Upon receiving a notification, the electronic device may extract a dynamic key component from the notification message and then access a static key component stored in the electronic device 230b. The dynamic key component and the static key component may be used to generate or compute a security key 240b which may be used to permit access of the electronic device to a database/server of downloadable information, firmware/software updates, additional network services, etc. The electronic device may send the generated security key to the server containing the information/update.

[0099] The security key (may also comprise the electronic device identification information or end user information) is examined and determined to be either authentic or inauthentic, i.e., verified or unverified 250b. The security key may also comprise, form example, electronic device identification information and/or end user information.

[00100] If the security key is determined to be inauthentic or unverified, then the electronic device may be denied access to the server 280b, and thus denied the ability to perform the download or update activity. However, if the security is determined to be authentic or verified, then the electronic device may be permitted access to the server

260b and the ability to download the update/service, etc. The electronic device may then retrieve the update package 266b and perform the update or modification 270b. In either situation, retrieval or abort, after completing the task, the electronic device may return to normal processing and wait for further notifications 210a.

[00101] Although a system and method according to the present invention has been described in connection with a preferred embodiment, it is not intended to be limited to the specific form set forth herein, but on the contrary, is intended to cover such alternatives, modifications, and equivalents, as can be reasonably included within the spirit and scope of the invention as defined by this disclosure and the appended diagrams. It is intended that the scope of the invention be limited not with this detailed description, but rather by the claims appended hereto.